UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/066,729	02/07/2002	Dae Hun Nyang	123056-05004486	4085

43569 7590 10/04/2005

MAYER, BROWN, ROWE & MAW LLP
1909 K STREET, N.W.
WASHINGTON, DC 20006

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 10/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/066,729	NYANG ET AL.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 July 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *2/7/02*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-13 have been presented for examination.

Information Disclosure Statement

2. The information disclosure statement filed 07 February 2002 fails to comply with 37 CFR 1.98(a)(3) because it does not include a concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR 1.56(c) most knowledgeable about the content of the information, of each patent listed that is not in the English language. It has been placed in the application file, but the information referred to therein has not been considered.

3. Furthermore, U.S. Patent No. 5,373,559 has been withdrawn and is unavailable to the Examiner. Therefore, it has been placed in the application file, but has not been considered.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claim 2 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 2 recites the limitation "its own password." It is unclear whose password the limitation is referring to.

6. Appropriate action is required.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1- 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Handbook of Applied Cryptography**, by Menezes et al., hereinafter Menezes, in view of **The Secure Remote Password Protocol**, by Thomas Wu, hereinafter Wu.

9. As per claim 1, Menezes teaches that zero-knowledge protocols require setting various kinds of system parameters for authentication as illustrated on page 408, Section **10.24 Protocol**, "One-time setup," page 410, Section **10.26 Protocol**, "Selection of System Parameters," page 412, Section **10.31 Protocol**, "Selection of System Parameters," and page 415, Section **10.36 Protocol** "Selection of System Parameters."

a user selecting a certain random number (r, x) in conformity with the set parameters (page 410, *Selection of per entity secrets*, each entity select random integers, p. 413, [prover] A selects a random secret integer, p. 415, [prover] A chooses a random r), and sending to a server a message (p. 410, A->B, p. 411, send [information] to *B*, p. 413 **10.31 Protocol** Step 3(1), p. 413, **Example 10.32** Step 4.(b), p. 415 **10.36 Protocol** Step 4(a), p. 415 **10.37 Example** Step 4(a)), including a user ID (p. 413, **10.31 Protocol** Step 3(1), p. 413 **10.32 Example** Step 4(b), p. 415 **10.36 Protocol** Steps 2(a) & 3(1)), and a first question number generation value X known only to the server and the user (p. 413, **10.31 Protocol** Step 3(1), p. 413 **10.32 Example** Step 4(b), p. 415 **10.36 Protocol** Steps 2(a) & 3(1));

a third step of the server sending to the user a message including a second question number generation value Y known only to the server and the user (p. 408 **10.24 Protocol** Steps 2(2) & 3(b), p. 410 **10.26 Protocol** Steps 3(2) & 4(b), p. 413 **10.31 Protocol** Steps 3(2) & 4(c), p. 415 **10.36 Protocol** Steps 3(2) & 4(b));

a fourth step of the user authenticating the server by verifying the authentication Auth, computing a resultant value c of a secret coin tossing (p. 406 **(i) interactive proof systems and zero-knowledge protocols**) known only to the server and the user and sending to the server a witness number B for user authentication (p. 408-409 **10.24 Protocol** Steps 2(3) & 3(c), p. 410-411 **10.26 Protocol** Steps 3(3) & 4(c)); and

10. Menezes does not disclose a test number (A=OWF(r)) to which a one-way function (OWF) is applied, a message including an authentication Auth of whether the server possesses a public key, a session key SK in a general zero-knowledge proof, and the server that stores a password verifier (V=OWF(f(P)) for the respective user verifying the witness number B using the test number A, the password verifier V, and the value c, and exchanging the session key SK by computing the session key SK.

11. Wu teaches a test number (A=OWF(r)) to which a one-way function (OWF) is applied (p. 7-8, p. 13- 15, **Sectoin 5 Optimizing SRP**), a message including an authentication Auth of whether the server possesses a public key (p. 13- 15, **Sectoin 5 Optimizing SRP**), a session key SK in a general zero-knowledge proof (p. 6-8 **3.2 SRP: An AKE construction**), and the server that stores a password verifier (V=OWF(f(P)) for the respective user verifying the witness number B using the test number A, the password verifier V, and the value c, and exchanging the session key SK by computing the session key SK (p. 6-8 **3.2 SRP: An AKE construction**).

12. Both Menezes and Wu disclose the use and implementation of zero-knowledge proofs.

13. It would have been obvious to one of ordinary skill in the art at the time the invention was made implement the key exchange protocol with the zero-knowledge proof, since Wu states in the Abstract that such a modification offers significantly improved performance over comparably strong extended methods that resist stolen-verifier attacks.

14. Regarding claim 2, Menezes teaches wherein the witness number B is sent to the server using the value c, the random number r (p. 408-409 **10.24 Protocol** Steps 2(3) & 3(c), p. 410-411 **10.26 Protocol** Steps 3(3) & 4(c)). Wu discloses incorporating a password P into zero-knowledge proofs (p. 4 – 8 **3 A new Framework**).

15. Regarding claim 3, Wu teaches wherein the user authenticates the server by confirming whether the server possesses the password verifier (p. 4 – 8 **3 A new Framework**).

16. Regarding claim 4, Menezes discloses wherein if the one-way function (p. 412 **10.30 Note**) is based on an RSA problem (p. 408 **10.24 Protocol** "trusted center publishes an RSA-like modulus), the password verifier is $V = [f(P^{-1})^e \mod n$, where $n = p*q$ (p and q are RSA Fractions), e (fraction) is a public key, and f(P) is a function for expanding the password P into lg(n) bits (p. 410 **10.26 Protocol**, p. 412-414 **10.31 Protocol**).

17. Regarding claim 5, Menezes discusses concatenation techniques on p. 412 **10.30 Note**. It would therefore have been obvious to have the witness number B is $B=r*f(P)^c \mod n$, where

c=H(TSK||A), TSK = H(K'||0), K = $[V^{-1}(Y)]^X$, and K' = $H(K||g^x||g^y||ID_{User}||ID_{Server})$, and H( ) is a hash function, since Menezes states that the bit size must be increased to preclude off-line dictionary attacks on the hash function.

18. Regarding claim 6, Menezes discusses concatenation techniques on p. 412 **10.30 Note**. It would therefore have been obvious to have the witness number B s performed using $B^e*V^C=A$ mod n where c=H(TSK||A), TSK=H(K'||0) K=$[V^{-1}(Y)]^X$ and K'=$H(K||g^X||g^Y||ID_{User}||ID_{Server})$, since Menezes states that the bit size must be increased to preclude off-line dictionary attacks on the hash function.

19. Regarding claim 7, Menezes discloses wherein if the one-way function is based on a discrete logarithm problem, the password verifier is $V=a^{-F(P)}$ mod p where a is a generator of Z^*_q, p is a fraction, and f(P) is a function for expanding the password P into lg(n) bits (p. 410 **10.26 Protocol**, p. 412-414 **10.31 Protocol**).

20. Regarding claim 8, Menezes discusses concatenation techniques on p. 412 **10.30 Note**. It would therefore have been obvious to have the witness number is B=r + f(P)*c mod q where c=H(TSK||A), TSK = H(K'||0), K = $[V^{-1}(Y)]^X$, and K' = $H(K||g^x||g^y||ID_{User}||ID_{Server})$, and H() is a hash function, since Menezes states that the bit size must be increased to preclude off-line dictionary attacks on the hash function.

21. With regards to claim 9, Menezes discusses concatenation techniques on p. 412 **10.30 Note**. It would therefore have been obvious to have the witness number B is performed using $a^B V^{C} = A \bmod p$, where c=H(TSK||A), TSK=H(K'||0) $K=[V^{-1}(Y)]^X$ and $K'=H(K||g^X||g^Y||ID_{User}||ID_{Server})$, since Menezes states that the bit size must be increased to preclude off-line dictionary attacks on the hash function.

22. Regarding claim 10, Menezes teaches wherein if the one-way function is based on a prime factorization problem, the password verifier is $[V_1 = [f(P+1)^{-1}]^2 \bmod n$, $V_2 = [f(P+2)^{-1}]^2 \bmod n$, $V_3 = [f(P+3)^{-1}]^2 \bmod n$, ..., $V_k = [f(P+k)^{-1}]^2 \bmod n$, $V = H(V_1, V_2, ..., V_k)]$, where $n = p*q$(p and q are RSA fractions), and f(P) is a function for expanding the password P into lg(n) bits (p. 410 **10.26 Protocol**, p. 412-414 **10.31 Protocol**).

23. Regarding claim 11, , Menezes discusses concatenation techniques on p. 412 **10.30 Note**. It would therefore have been obvious to have the witness number is $B = r * \prod f(P + i)^{Ci}$ where c=H(TSK||A), TSK = H(K'||0), $K = [V^{-1}(Y)]^X$, and $K' = H(K||g^x||g^y||ID_{User}||ID_{Server})$, and H( ) is a hash function, since Menezes states that the bit size must be increased to preclude off-line dictionary attacks on the hash function.

24. With regards to claim 12, Menezes discusses concatenation techniques on p. 412 **10.30 Note**. It would therefore have been obvious to have the witness number B is performed using $A = B^2 * \prod V_i^{Ci}$ where c=H(TSK||A), TSK=H(K'||0) $K=[V^{-1}(Y)]^X$ and

$K'=H(K||g^X||g^Y||ID_{User}||ID_{Server})$, and C_i is an i-th bit, since Menezes states that the bit size must be increased to preclude off-line dictionary attacks on the hash function.

25. Regarding claim 13, Menezes teaches wherein the server makes a random challenge transmitted for authentication from the server to the user known only to the server and the user to defend against an offline dictionary attack (p. 419-420 **(ii) Security level required for on-line vs. off-line attacks**).

Double Patenting

26. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

27. A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

28. Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

29. Claims 1-13 are provisionally rejected under the judicially created doctrine of double patenting over claims 1-3 of copending Application No. 10/641,618. This is a provisional double patenting rejection since the conflicting claims have not yet been patented.

30. The subject matter claimed in the instant application is fully disclosed in the referenced copending application and would be covered by any patent granted on that copending application since the referenced copending application and the instant application are claiming common subject matter, as follows:

31. Claim 1 of the instant application reads as follows:

a method of designing a password-based authentication and key exchange protocol using a zero-knowledge interactive proof, comprising:

a first step of setting various kinds of system parameters required for authentication;

a second step of a user selecting a certain random number (r, x) in conformity with the set parameters, and sending to a server a message including a user ID, a test number (A=OWF(r)) to which a one-way function (OWF) is applied, and a first question number generation value X known only to the server and the user;

a third step of the server sending to the user a message including an authentication Auth of whether the server possesses a public key, and a second question number generation value Y known only to the server and the user;

a fourth step of the user authenticating the server by verifying the authentication Auth, computing a resultant value c of a secret coin tossing known only to the server and the user and a session key SK in a general zero-knowledge proof, and sending to the server a witness number B for user authentication; and

a fifth step of the server that stores a password verifier (V=OWF(f(P)) for the respective user verifying the witness number B using the test number A, the password verifier V, and the value c, and exchanging the session key SK by computing the session key SK.

32. Claim 1 and 3 of the co-pending application recite the limitations:

a method for authenticating a user on a communization network containing a user computer and an authentication server, comprising the steps of:

a) setting up a variety of system parameters needed to perform an authentication process;

b) enabling a user to select an arbitrary random number (r) based on the setup system parameters, and transmitting to the authentication server a message composed of a test number A= Γ (r) being a result of applying a one-way function to a user ID and the random number (r)

c) after performing the step performing (b), performing a symmetric authenticated key exchange operation between the user computer authentication server, authenticating the authentication server, and allowing both the authentication server and the user computer to share a temporary session key (tsk);

d) after performing the step (c), enabling the authentication server to create a random number (t), and transmitting the random number (t) to the user computer;

e) enabling the user computer to create a question number (c) using the random number (t) and the temporary session key (tsk), calculating a witness number B using the question number (c), and transmitting the witness number B to the authentication server;

f) enabling the authentication server to verify the witness number B using the arbitrary session key (tsk), the test number A, and a KV (Key Verifier), etc; and

g) if successful verification performed in the step (f), enabling the authentication server and the user computer each to calculate a session key (sk).

33. Furthermore, there is no apparent reason why applicant would be prevented from presenting claims corresponding to those of the instant application in the other copending application. See *In re Schneller*, 397 F.2d 350, 158 USPQ 210 (CCPA 1968). See also MPEP § 804.

Conclusion

34. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

35. The following patents are cited to further show the state of the art with respect to zero-knowledge proofs, such as:

United States Patent No. 6,678,665 to Benson et al., which is cited to show using a zero-knowledge proof for protecting software.

United States Patent No. 5,483,597 to Stern, which is cited to show a zero-knowledge protocol for device identification.

United States Patent No. 5,841,869 to Merkling et al., which is cited to show using a zero-knowledge protocol for establishing a session key.

United States Patent No. 6,651,167 to Terao et al., which is cited to show a zero-knowledge protocol that uses a hash function.

United States Patent No. 6,567,916 to Terao et al., which is cited to show a zero-knowledge protocol that uses a hash function.

United States Patent No. 5,633,929 to Kaliski, Jr., which is cited to show interactive zero-knowledge protocols.

United States Patent No. 6,125,445 to Arditti et al., which is cited to show zero-knowledge protocols using public key identification processes.

36. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

37. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

38. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131

clf

Primary Examiner
AU 2131
9/29/05